

CLAIMS

What is claimed is:

1. A method comprising:

selecting an elliptic curve;

determining a Squared Weil pairing based on said elliptic curve; and

cryptographically processing selected information based on said Squared Weil pairing.

2. The method as recited in Claim 1, wherein said elliptic curve includes an elliptic curve E over a field K , wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

3. The method as recited in Claim 2, wherein determining said Squared Weil pairing based on said elliptic curve further includes establishing a point **id** that is defined as a point at infinity on E , and wherein **P**, **Q**, **R**, **X** are points on E wherein **X** is an indeterminate denoting an independent variable of a function, and wherein $x(\mathbf{X})$, $y(\mathbf{X})$ are functions mapping said point **X** on E to its affine x and y coordinates, and wherein a line passes through said points **P**, **Q**, **R** if $\mathbf{P} + \mathbf{Q} + \mathbf{R} = \mathbf{id}$.

4. The method as recited in Claim 3, wherein when at least two of said **P**, **Q**, **R** points are equal, said line is a tangent line at a common point.

1 5. The method as recited in Claim 3, wherein determining said Squared
2 Weil pairing based on said elliptic curve further includes:

3 with a first function f_j, \mathbf{P} and a second function f_k, \mathbf{P} for two integers j and k ,
4 deriving a third function f_{-j-k}, \mathbf{P} based on said first and second functions.

5
6 6. The method as recited in Claim 5, wherein $(f_{-j-k}, \mathbf{P} f_j, \mathbf{P} f_k, \mathbf{P}) = (f_{-j-k}, \mathbf{P})$
7 $+ (f_j, \mathbf{P}) + (f_k, \mathbf{P}) = 3(\mathbf{id}) - ((-j-k)\mathbf{P}) - (j\mathbf{P}) - (k\mathbf{P})$.

8
9 7. The method as recited in Claim 5, wherein $f_{-j-k}, \mathbf{P}(\mathbf{X}) f_j, \mathbf{P}(\mathbf{X}) f_k, \mathbf{P}(\mathbf{X})$
10 $\text{line}(j\mathbf{P}, k\mathbf{P}, (-j-k)\mathbf{P})(\mathbf{X}) = \text{a constant}$.

11
12 8. The method as recited in Claim 5, wherein if j is an integer and \mathbf{P} a
13 point on E , then said first and second functions are rational functions on E whose
14 divisor of zeros and poles is $(f_j, \mathbf{P}) = j(\mathbf{P}) - (j\mathbf{P}) - (j-1)(\mathbf{id})$.

15
16 9. The method as recited in Claim 8, wherein if $j > 1$ and $\mathbf{P}, j\mathbf{P}$, and \mathbf{id}
17 are distinct, then said first function has a j -fold zero at $\mathbf{X} = \mathbf{P}$, a simple pole at $\mathbf{X} =$
18 $j\mathbf{P}$, a $(j-1)$ -fold pole at infinity, and no other poles or zeros.

19
20 10. The method as recited in Claim 8, wherein if j equals 0 or 1 then said
21 first function is a nonzero constant.

22
23 11. The method as recited in Claim 5, further comprising determining
24 $f_{0, \mathbf{P}}$ such that a line through $0\mathbf{P} = \mathbf{id}$, $(-j-k)\mathbf{P}$, and $(j+k)\mathbf{P}$ is vertical in that its
25 equation does not reference a y -coordinate.

12. The method as recited in Claim 11, wherein:

$$f_{j+k, \mathbf{P}}(\mathbf{X}) = f_{j, \mathbf{P}}(\mathbf{X}) f_{k, \mathbf{P}}(\mathbf{X}) \frac{\text{line}(j\mathbf{P}, k\mathbf{P}, (-j-k)\mathbf{P})(\mathbf{X})}{\text{line}(\mathbf{id}, (-j-k)\mathbf{P}, (j+k)\mathbf{P})(\mathbf{X})}, \text{ and}$$

$$f_{j-k, \mathbf{P}}(\mathbf{X}) = \frac{f_{j, \mathbf{P}}(\mathbf{X}) \text{line}(\mathbf{id}, j\mathbf{P}, -j\mathbf{P})(\mathbf{X})}{f_{k, \mathbf{P}}(\mathbf{X}) \text{line}(-j\mathbf{P}, k\mathbf{P}, (j-k)\mathbf{P})(\mathbf{X})}.$$

13. The method as recited in Claim 11, wherein:

$$f_{j, \mathbf{id}} = \text{constant};$$

$$f_{j, -\mathbf{P}}(\mathbf{X}) = f_{j, \mathbf{P}}(-\mathbf{X}) * (\text{constant}); \text{ and}$$

if $(\mathbf{P} + \mathbf{Q} + \mathbf{R} = \mathbf{id})$, then:

$$f_{j, \mathbf{P}}(\mathbf{X}) f_{j, \mathbf{Q}}(\mathbf{X}) f_{j, \mathbf{R}}(\mathbf{X}) = \frac{\text{line}(\mathbf{P}, \mathbf{Q}, \mathbf{R})(\mathbf{X})^j}{\text{line}(j\mathbf{P}, j\mathbf{Q}, j\mathbf{R})(\mathbf{X})}.$$

14. The method as recited in Claim 3, wherein \mathbf{P} and \mathbf{Q} are m -torsion points on E and m is an odd prime, and wherein determining said Squared Weil pairing further includes:

determining said squared Weil pairing based on

$$\frac{f_{m, \mathbf{P}}(\mathbf{Q}) f_{m, \mathbf{Q}}(-\mathbf{P})}{f_{m, \mathbf{P}}(-\mathbf{Q}) f_{m, \mathbf{Q}}(\mathbf{P})} = -e_m(\mathbf{P}, \mathbf{Q})^2,$$

where e_m denotes the Weil-pairing.

15. The method as recited in Claim 14, wherein neither \mathbf{P} nor \mathbf{Q} is an identity and \mathbf{P} is not equal to $\pm \mathbf{Q}$.

1 16. A computer-readable medium having computer-implementable
2 instructions for causing at least one processing unit to perform acts comprising:
3 determining a Squared Weil pairing based on an elliptic curve; and
4 cryptographically processing selected information based on said Squared
5 Weil pairing.

6
7 17. The computer-readable medium as recited in Claim 16, wherein said
8 elliptic curve includes an elliptic curve E over a field K , wherein E can be
9 represented as an equation $y^2 = x^3 + ax + b$.

10
11 18. The computer-readable medium as recited in Claim 17, determining
12 said Squared Weil pairing based on said elliptic curve further includes establishing
13 a point **id** that is defined as a point at infinity on E , and wherein **P**, **Q**, **R**, **X** are
14 points on E wherein **X** is an indeterminate denoting an independent variable of a
15 function, and wherein $x(\mathbf{X})$, $y(\mathbf{X})$ are functions mapping said point **X** on E to its
16 affine x and y coordinates, and wherein a line passes through said points **P**, **Q**, **R**
17 if **P + Q + R = id**.

18
19 19. The computer-readable medium as recited in Claim 18, wherein
20 determining said Squared Weil pairing based on said elliptic curve further
21 includes:

22 determining a first function $f_{j,\mathbf{P}}$ and a second function $f_{k,\mathbf{P}}$ for two integers j
23 and k ; and

24 determining a third function $f_{-j-k,\mathbf{P}}$ based on said first and second functions.
25

20. The computer-readable medium as recited in Claim 19, wherein
 $(f_{-j-k,\mathbf{P}} f_{j,\mathbf{P}} f_{k,\mathbf{P}}) = (f_{-j-k,\mathbf{P}}) + (f_{j,\mathbf{P}}) + (f_{k,\mathbf{P}}) = 3(\mathbf{id}) - ((-j-k)\mathbf{P}) - (j\mathbf{P}) - (k\mathbf{P})$.

21. The computer-readable medium as recited in Claim 20, wherein
 $f_{-j-k,\mathbf{P}}(\mathbf{X}) f_{j,\mathbf{P}}(\mathbf{X}) f_{k,\mathbf{P}}(\mathbf{X}) \text{line}(j\mathbf{P}, k\mathbf{P}, (-j-k)\mathbf{P})(\mathbf{X}) = \text{a constant}$.

22. The computer-readable medium as recited in Claim 20, wherein if j
 is an integer and \mathbf{P} a point on E , then said first and second functions *are* rational
 functions on E whose divisor of zeros and poles is $(f_{j,\mathbf{P}}) = j(\mathbf{P}) - (j\mathbf{P}) - (j-1)(\mathbf{id})$.

23. The computer-readable medium as recited in Claim 20, further
 comprising determining $f_{0,\mathbf{P}}$ such that a line through $0\mathbf{P} = \mathbf{id}$, $(-j-k)\mathbf{P}$, and $(j+k)\mathbf{P}$
 is vertical in that it does not reference a y -coordinate.

24. The computer-readable medium as recited in Claim 23, wherein:

$$f_{j+k,\mathbf{P}}(\mathbf{X}) = f_{j,\mathbf{P}}(\mathbf{X}) f_{k,\mathbf{P}}(\mathbf{X}) \frac{\text{line}(j\mathbf{P}, k\mathbf{P}, (-j-k)\mathbf{P})(\mathbf{X})}{\text{line}(\mathbf{id}, (-j-k)\mathbf{P}, (j+k)\mathbf{P})(\mathbf{X})}, \text{ and}$$

$$f_{j-k,\mathbf{P}}(\mathbf{X}) = \frac{f_{j,\mathbf{P}}(\mathbf{X}) \text{line}(\mathbf{id}, j\mathbf{P}, -j\mathbf{P})(\mathbf{X})}{f_{k,\mathbf{P}}(\mathbf{X}) \text{line}(-j\mathbf{P}, k\mathbf{P}, (j-k)\mathbf{P})(\mathbf{X})}.$$

1 25. The computer-readable medium as recited in Claim 23, wherein:

2 $f_{j,\mathbf{id}} = \text{constant}$;

3 $f_{j,-\mathbf{P}}(\mathbf{X}) = f_{j,\mathbf{P}}(-\mathbf{X}) * (\text{constant})$; and

4 if $(\mathbf{P} + \mathbf{Q} + \mathbf{R} = \mathbf{id})$, then:

5
$$f_{j,\mathbf{P}}(\mathbf{X}) f_{j,\mathbf{Q}}(\mathbf{X}) f_{j,\mathbf{R}}(\mathbf{X}) = \frac{\text{line}(\mathbf{P}, \mathbf{Q}, \mathbf{R})(\mathbf{X})^j}{\text{line}(j\mathbf{P}, j\mathbf{Q}, j\mathbf{R})(\mathbf{X})}.$$

6

7

8 26. The computer-readable medium as recited in Claim 18, wherein \mathbf{P}
9 and \mathbf{Q} are m -torsion points on E and m is an odd prime, and wherein determining
10 said Squared Weil pairing further includes:

11 determining said squared Weil pairing based on

12

13
$$\frac{f_{m,\mathbf{P}}(\mathbf{Q}) f_{m,\mathbf{Q}}(-\mathbf{P})}{f_{m,\mathbf{P}}(-\mathbf{Q}) f_{m,\mathbf{Q}}(\mathbf{P})} = -e_m(\mathbf{P}, \mathbf{Q})^2,$$

14

15 where e_m denotes the Weil-pairing.

16

17 27. An apparatus comprising:

18 memory configured to store information suitable for use with using a
19 cryptographic process;

20 logic operatively coupled to said memory and configured to determine a
21 Squared Weil pairing based on at least one elliptic curve, and cryptographically
22 process selected information stored in said memory based on said Squared Weil
23 pairing.

24

25

1 28. The apparatus as recited in Claim 27, wherein said logic is further
2 configured to determine said elliptic curve, which includes an elliptic curve E over
3 a field K , wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

4
5 29. The apparatus as recited in Claim 27, wherein said logic is further
6 configured to establishing a point **id** that is defined as a point at infinity on E , and
7 wherein **P**, **Q**, **R**, **X** are points on E wherein **X** is an indeterminate denoting an
8 independent variable of a function, and wherein $x(\mathbf{X})$, $y(\mathbf{X})$ are functions mapping
9 said point **X** on E to its affine x and y coordinates, and wherein a line passes
10 through said points **P**, **Q**, **R** if $\mathbf{P} + \mathbf{Q} + \mathbf{R} = \mathbf{id}$.

11
12 30. The apparatus as recited in Claim 29, wherein said logic is further
13 configured to determine a first function $f_{j,\mathbf{P}}$ and a second function $f_{k,\mathbf{P}}$ for two
14 integers j and k , and a third function $f_{-j-k,\mathbf{P}}$ based on said first and second
15 functions.

16
17 31. The apparatus as recited in Claim 30, wherein $(f_{-j-k,\mathbf{P}} f_{j,\mathbf{P}} f_{k,\mathbf{P}}) =$
18 $(f_{-j-k,\mathbf{P}}) + (f_{j,\mathbf{P}}) + (f_{k,\mathbf{P}}) = 3(\mathbf{id}) - ((-j-k)\mathbf{P}) - (j\mathbf{P}) - (k\mathbf{P})$.

19
20 32. The apparatus as recited in Claim 30, wherein $f_{-j-k,\mathbf{P}}(\mathbf{X}) f_{j,\mathbf{P}}(\mathbf{X}) f_{k,\mathbf{P}}$
21 $(\mathbf{X}) \text{ line}(j\mathbf{P}, k\mathbf{P}, (-j-k)\mathbf{P})(\mathbf{X}) = \text{a constant}$.

22
23 33. The apparatus as recited in Claim 30, wherein if j is an integer and **P**
24 a point on E , then said first and second functions are rational functions on E whose
25 divisor of zeros and poles is $(f_{j,\mathbf{P}}) = j(\mathbf{P}) - (j\mathbf{P}) - (j-1)(\mathbf{id})$.

34. The apparatus as recited in Claim 30, wherein said logic is further configured to determine $f_{0,\mathbf{P}}$ such that a line through $0\mathbf{P} = \mathbf{id}$, $(-j-k)\mathbf{P}$, and $(j+k)\mathbf{P}$ is vertical in that it does not reference a y -coordinate.

35. The apparatus as recited in Claim 34, wherein:

$$f_{j+k,\mathbf{P}}(\mathbf{X}) = f_{j,\mathbf{P}}(\mathbf{X})f_{k,\mathbf{P}}(\mathbf{X}) \frac{\text{line}(\mathbf{jP}, \mathbf{kP}, (-j-k)\mathbf{P})(\mathbf{X})}{\text{line}(\mathbf{id}, (-j-k)\mathbf{P}, (j+k)\mathbf{P})(\mathbf{X})}, \text{ and}$$

$$f_{j-k,\mathbf{P}}(\mathbf{X}) = \frac{f_{j,\mathbf{P}}(\mathbf{X})\text{line}(\mathbf{id}, \mathbf{jP}, -\mathbf{jP})(\mathbf{X})}{f_{k,\mathbf{P}}(\mathbf{X})\text{line}(-\mathbf{jP}, \mathbf{kP}, (j-k)\mathbf{P})(\mathbf{X})}.$$

36. The apparatus as recited in Claim 34, wherein:

$$f_{j,\mathbf{id}} = \text{constant};$$

$$f_{j,-\mathbf{P}}(\mathbf{X}) = f_{j,\mathbf{P}}(-\mathbf{X}) * (\text{constant}); \text{ and}$$

if $(\mathbf{P} + \mathbf{Q} + \mathbf{R} = \mathbf{id})$, then:

$$f_{j,\mathbf{P}}(\mathbf{X})f_{j,\mathbf{Q}}(\mathbf{X})f_{j,\mathbf{R}}(\mathbf{X}) = \frac{\text{line}(\mathbf{P}, \mathbf{Q}, \mathbf{R})(\mathbf{X})^j}{\text{line}(\mathbf{jP}, \mathbf{jQ}, \mathbf{jR})(\mathbf{X})}.$$

37. The apparatus as recited in Claim 30, wherein \mathbf{P} and \mathbf{Q} are m -torsion points on E and m is an odd prime, and wherein said logic is further configured to determine said squared Weil pairing based on

$$\frac{f_{m,\mathbf{P}}(\mathbf{Q})f_{m,\mathbf{Q}}(-\mathbf{P})}{f_{m,\mathbf{P}}(-\mathbf{Q})f_{m,\mathbf{Q}}(\mathbf{P})} = -e_m(\mathbf{P}, \mathbf{Q})^2,$$

where e_m denotes the Weil-pairing.

1 38. A method comprising:

2 determining a Squared Weil Pairing $e_m(\mathbf{P}, \mathbf{Q})^2$ by:

3 establishing an odd prime m on a curve E ; *and*

4 based on two m -torsion points \mathbf{P} and \mathbf{Q} on E , computing $e_m(\mathbf{P}, \mathbf{Q})^2$.

5
6 39. The method as recited in Claim 38, further comprising forming a
7 mathematical chain for m .

8
9 40. The method as recited in Claim 39, wherein said mathematical chain
10 is selected from a group of mathematical chains comprising an addition chain and
11 an addition-subtraction chain.

12
13 41. The method as recited in Claim 39, wherein in forming said
14 mathematical chain for m , every element in said mathematical chain is a sum or
15 difference of two earlier elements in said mathematical chain, which continues
16 until m is included in said mathematical chain.

17
18 42. The method as recited in Claim 41, wherein said mathematical chain
19 has a length $O(\log(m))$.

20
21 43. The method as recited in Claim 39, wherein for each j in said
22 mathematical chain, a tuple $t_j = [j\mathbf{P}, j\mathbf{Q}, n_j, d_j]$ is formed such that

23
$$\frac{n_j}{d_j} = \frac{f_{j,\mathbf{P}}(\mathbf{Q})f_{j,\mathbf{Q}}(-\mathbf{P})}{f_{j,\mathbf{P}}(-\mathbf{Q})f_{j,\mathbf{Q}}(\mathbf{P})}.$$

1 44. The method as recited in Claim 43, wherein determining said
2 Squared Weil Pairing further includes:

3 starting with $t_1 = [\mathbf{P}, \mathbf{Q}, 1, 1]$, given t_j and t_k , determine t_{j+k} by:

4 forming elliptic curve sums: $j\mathbf{P} + k\mathbf{P} = (j+k)\mathbf{P}$ and $j\mathbf{Q} + k\mathbf{Q} =$
5 $(j+k)\mathbf{Q}$;

6 determining $\text{line}(j\mathbf{P}, k\mathbf{P}, (-j-k)\mathbf{P})(\mathbf{X}) = c0 + c1 * x(\mathbf{X}) + c2 * y(\mathbf{X})$;

7 determining $\text{line}(j\mathbf{Q}, k\mathbf{Q}, (-j-k)\mathbf{Q})(\mathbf{X}) = c0' + c1' * x(\mathbf{X}) + c2' * y(\mathbf{X})$;

8 and

9 setting

10
$$n_{j+k} = n_j * n_k * (c0 + c1 * x(\mathbf{Q}) + c2 * y(\mathbf{Q})) * (c0' + c1' * x(\mathbf{P}) - c2' * y(\mathbf{P}))$$

11 and

12
$$d_{j+k} = d_j * d_k * (c0 + c1 * x(\mathbf{Q}) - c2 * y(\mathbf{Q})) * (c0' + c1' * x(\mathbf{P}) + c2' * y(\mathbf{P})).$$

13
14 45. The method as recited in Claim 44, further comprising determining
15 t_{j+k} from t_j and t_k , wherein vertical lines through $(j+k)\mathbf{P}$ and $(j+k)\mathbf{Q}$ do not appear
16 in said formulae for n_{j+k} and d_{j+k} when contributions from \mathbf{Q} and $-\mathbf{Q}$ are equal,
17 and wherein $-\mathbf{Q}$ is the complement of \mathbf{Q} and when contributions from \mathbf{P} and $-\mathbf{P}$
18 are equal, and wherein $-\mathbf{P}$ is the complement of \mathbf{P} .

19
20 46. The method as recited in Claim 44, wherein if $j + k = m$, then $n_{j+k} =$
21 $n_j * n_k$ and $d_{j+k} = d_j * d_k$.

1 47. A computer-readable medium having computer-implementable
2 instructions for causing at least one processing unit to perform acts comprising:

3 determining a Squared Weil Pairing $e_m(\mathbf{P}, \mathbf{Q})^2$ by:

4 establishing an odd prime m on a curve E ; and

5 based on two m -torsion points \mathbf{P} and \mathbf{Q} on E , computing $e_m(\mathbf{P}, \mathbf{Q})^2$.

6
7 48. The computer-readable medium as recited in Claim 47, further
8 comprising forming a mathematical chain for m selected from a group of
9 mathematical chains comprising an addition chain and an addition-subtraction
10 chain, such that every element in said mathematical chain is a sum or difference of
11 two earlier elements in said mathematical chain, which continues until m is
12 included in said mathematical chain.

13
14 49. The computer-readable medium as recited in Claim 48, wherein for
15 each j in said mathematical chain, a tuple $t_j = [j\mathbf{P}, j\mathbf{Q}, n_j, d_j]$ is formed such that

16
$$\frac{n_j}{d_j} = \frac{f_{j,\mathbf{P}}(\mathbf{Q})f_{j,\mathbf{Q}}(-\mathbf{P})}{f_{j,\mathbf{P}}(-\mathbf{Q})f_{j,\mathbf{Q}}(\mathbf{P})}.$$

17
18
19 50. An apparatus comprising:
20 memory configured to store information suitable for use with using a
21 cryptographic process;

22 logic operatively coupled to said memory and configured to determine a
23 Squared Weil Pairing $e_m(\mathbf{P}, \mathbf{Q})^2$ by establishing an odd prime m on a curve E , and
24 based on two m -torsion points \mathbf{P} and \mathbf{Q} on E , computing $e_m(\mathbf{P}, \mathbf{Q})^2$.

51. The apparatus as recited in Claim 50, wherein said logic is further configured to form a mathematical chain for m that is selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain.

52. The apparatus as recited in Claim 51, wherein for each j in said mathematical chain, said logic is further configured to form a tuple $t_j = [j\mathbf{P}, j\mathbf{Q}, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,\mathbf{P}}(\mathbf{Q})f_{j,\mathbf{Q}}(-\mathbf{P})}{f_{j,\mathbf{P}}(-\mathbf{Q})f_{j,\mathbf{Q}}(\mathbf{P})}.$$

53. A method comprising:

determining a Squared Weil pairing $(m, \mathbf{P}, \mathbf{Q})$, where m is an odd prime number, by setting $t_1 = [\mathbf{P}, \mathbf{Q}, 1, 1]$, using an addition-subtraction chain to determine $t_m = [m\mathbf{P}, m\mathbf{Q}, n_m, d_m]$, and if n_m and d_m are nonzero, then determining:

$$\frac{n_m}{d_m} = \frac{f_{m,\mathbf{P}}(\mathbf{Q})f_{m,\mathbf{Q}}(-\mathbf{P})}{f_{m,\mathbf{P}}(-\mathbf{Q})f_{m,\mathbf{Q}}(\mathbf{P})}; \text{ and}$$

cryptographically processing selected information based on said Squared Weil pairing.

1 56. A method comprising:
2 selecting an elliptic curve;
3 determining a Squared Tate pairing based on said elliptic curve; and
4 cryptographically processing selected information based on said Squared
5 Tate pairing.

6
7 57. The method as recited in Claim 56, wherein said elliptic curve
8 includes an elliptic curve E over a field K , wherein E can be represented as an
9 equation $y^2 = x^3 + ax + b$.

10
11 58. The method as recited in Claim 56, wherein m is an odd prime on K
12 and P is an m -torsion point on E , Q is a point on E , with neither \mathbf{P} nor \mathbf{Q} being the
13 identity and wherein \mathbf{P} is not equal to a multiple of \mathbf{Q} , and wherein E is defined
14 over K , K has $q = p^n$ elements, and m divides $q-1$, then determining that

$$\left(\frac{f_{m,\mathbf{P}}(\mathbf{Q})}{f_{m,\mathbf{P}}(-\mathbf{Q})} \right)^{\frac{q-1}{m}} = v_m(\mathbf{P}, \mathbf{Q}),$$

17 where v_m denotes the squared Tate-pairing.

59. The method as recited in Claim 56, wherein determining said Squared Tate pairing includes determining $v_m(\mathbf{P}, \mathbf{Q})$ by:

establishing an odd prime m and said elliptic curve E ;

given an m -torsion point \mathbf{P} on E and a point \mathbf{Q} on E , determining a mathematical chain for m ; and

for each j in said mathematical chain, forming a tuple $t_j = [j\mathbf{P}, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,\mathbf{P}}(\mathbf{Q})}{f_{j,\mathbf{P}}(-\mathbf{Q})}.$$

60. The method as recited in Claim 59, further comprising:

starting with $t_1 = [\mathbf{P}, 1, 1]$, given t_j and t_k , determining t_{j+k} by:

forming an elliptic curve sum $j\mathbf{P} + k\mathbf{P} = (j+k)\mathbf{P}$,

determining $\text{line}(j\mathbf{P}, k\mathbf{P}, (-j-k)\mathbf{P})(\mathbf{X}) = c_0 + c_1 * x(\mathbf{X}) + c_2 * y(\mathbf{X})$,

and

setting: $n_{j+k} = n_j * n_k * (c_0 + c_1 * x(\mathbf{Q}) + c_2 * y(\mathbf{Q}))$ and

$$d_{j+k} = d_j * d_k * (c_0 + c_1 * x(\mathbf{Q}) - c_2 * y(\mathbf{Q})).$$

61. The method as recited in Claim 60 further comprising determining t_{j-k} from t_j and t_k .

62. The method as recited in Claim 61, wherein if $j+k=m$, then:

$$n_{j+k} = n_j * n_k \text{ and } d_{j+k} = d_j * d_k.$$

1 63. The method as recited in Claim 61, wherein if n_m and d_m are
2 nonzero, then:

3
$$\frac{n_m}{d_m} = \frac{f_{m,P}(Q)}{f_{m,P}(-Q)}.$$

4

5
6 64. The method as recited in Claim 56, wherein said mathematical chain
7 is selected from a group of mathematical chains comprising an addition chain and
8 an addition-subtraction chain.

9
10 65. A computer-readable medium having computer-implementable
11 instructions for causing at least one processing unit to perform acts comprising:
12 determining a Squared Tate pairing based on an elliptic curve; and
13 cryptographically processing selected information based on said Squared
14 Tate pairing.

15
16 66. The computer-readable medium as recited in Claim 65, wherein said
17 elliptic curve includes an elliptic curve E over a field K , wherein E can be
18 represented as an equation $y^2 = x^3 + ax + b$.

67. The computer-readable medium as recited in Claim 65, wherein m is an odd prime on K and P is an m -torsion point on E , Q is a point on E , with neither P nor Q being the identity and wherein P is not equal to a multiple of Q , and wherein E is defined over K , K has $q = p^n$ elements, and m divides $q-1$, then determining that

$$\left(\frac{f_{m,P}(Q)}{f_{m,P}(-Q)} \right)^{\frac{q-1}{m}} = v_m(P, Q),$$

where v_m denotes the squared Tate-pairing.

68. The computer-readable medium as recited in Claim 65, wherein determining said Squared Tate pairing includes determining $v_m(P, Q)$ by:

establishing an odd prime m and said elliptic curve E ;

given an m -torsion point P on E and a point Q on E , determining a mathematical chain for m ; and

for each j in said mathematical chain, forming a tuple $t_j = [jP, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,P}(Q)}{f_{j,P}(-Q)}.$$

69. An apparatus comprising:
memory configured to store information suitable for use with using a
cryptographic process;
logic operatively coupled to said memory and configured to determine a
Squared Tate pairing based on an elliptic curve; and
cryptographically processing selected information based on said Squared
Tate pairing.

70. The apparatus as recited in Claim 69, wherein said elliptic curve
includes an elliptic curve E over a field K , wherein E can be represented as an
equation $y^2 = x^3 + ax + b$.

71. The apparatus as recited in Claim 69 wherein m is an odd prime on
 K and P is an m -torsion point on E , Q is a point on E , with neither P nor Q being
the identity and wherein P is not equal to a multiple of Q , and wherein E is
defined over K , K has $q = p^n$ elements, and m divides $q-1$, then determining that

$$\left(\frac{f_{m,P}(Q)}{f_{m,P}(-Q)} \right)^{\frac{q-1}{m}} = v_m(P, Q),$$

where v_m denotes the squared Tate-pairing.

1 72. The apparatus as recited in Claim 69, wherein said logic is further
2 configured to:

3 establish an odd prime m and said elliptic curve E ;

4 given an m -torsion point \mathbf{P} on E and a point \mathbf{Q} on E , determine a
5 mathematical chain for m ; and

6 for each j in said mathematical chain, form a tuple $t_j = [j\mathbf{P}, n_j, d_j]$ such that

7
$$\frac{n_j}{d_j} = \frac{f_{j,\mathbf{P}}(\mathbf{Q})}{f_{j,\mathbf{P}}(-\mathbf{Q})}.$$

8